Claims

1. Mobile telephone handset (1), characterised in that it comprises:

- a storage support (2) which is secured against fraudulent access, which stores the IMEI (21) of the handset;

- a connector (3) for a secure electronic module (31), which is associated with an operator;

- a handset (1) operating system (4), which controls authentication of the IMEI storage support (2) by a secure electronic module which is connected to the aforementioned connector in order to establish a secure communication channel (6) between the storage support and the module and transmission of the IMEI over the secure channel to the secure electronic module.

2. Mobile telephone handset (1) according to claim 1, characterised in that the operating system (4) controls the transmission of the IMEI to a mobile telephone operator (5) by means of a secure OTA channel.

3. Handset according to any one of the preceding claims, characterised in that it comprises a secure electronic module (31) associated with the operator connected to the connector.

4. Handset according to claim 3, characterised in that the secure electronic module is a UICC.

5. Handset according to claim 3 or 4, characterised in that the operating system controls the

authentication of the secure module by the storage support.

6. Handset according to claim 5, characterised in that the secure electronic module and the storage support store encryption keys (22) that are adapted to securing the secure communication channel (6).

7. Handset according to any one of the claims from 3 to 6, characterised in that the secure module (31) blocks the use of the handset when a false IMEI is detected.

8. Method of securing the IMEI of a mobile telephone handset (1) comprising the following steps:

- authenticating a secure storage support by memorising its IMEI (21), by a secure electronic module (31) associated with the operator and inserted in a connector (3) of the handset, in order to establish a secure channel between the storage support and the secure module;

- transmitting the IMEI (21) from the storage support to the secure module over the secure channel.

9. Method according to claim 8, characterised in that the secure module (31) also transmits the IMEI to a mobile telephone operator over a secure OTA channel.

10. Method according to claim 9, characterised in that the operator compares the IMEI with a black list (7) of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

11. Method according to any one of the claims from 8 to 10, characterised in that the secure module

blocks the use of the handset when a false IMEI is detected.